Die Corona-Warn-App unter der Lupe

FALK SIPPACH

JUG Saxony Day Online 2021

Freitag, 01.10.2021

embarc
Software Consulting GmbH

1

Die Corona-Warn-App unter der Lupe

Zusammenfassung

Leuchtturmprojekt, Kostengrab, Hoffnungsträger und wichtiger Baustein in der Pandemiebekämpfung - das deutsche Corona-Warn-App-System (kurz CWA) besteht nicht nur aus den recht prominenten iOS- und Android-Apps. Zur Umsetzung von Use Cases wie der persönlichen Risikoermitttlung oder dem Melden von (positiven) Testergebnissen, gehört auch eine vielteilige Server-Lösung. Sie basiert auf einem zeitgemäßen Architekturstil und einem aktuellen Technologie-Stack. Und wurde unter hohem Zeitdruck federführend von SAP und Deutscher Telekom realisiert.

Das öffentliche Interesse an diesem Projekt ist hoch, die Transparenz bei der Entwicklung erfreulicherweise ebenfalls. Der Quellcode ist Open Source und auch die Dokumentation offen zugänglich. Wir diskutieren die prägenden architekturrelevanten Anforderungen und die getroffenen Entscheidungen. Zum Abschluss bewerten wir die gewählten Lösungsansätze und arbeiten Stärken, Hindernisse und Kompromisse heraus.

2

Falk Sippach

- Softwarearchitekt, Berater, Trainer bei embarc
- früher bei Orientation in Objects (OIO), Trivadis

Schwerpunkte:

- Architekturberatung und -bewertung
- Cloud- und Java-Technologien

fs@embarc.de

@sippsack

➔ xing.to/fsi

embarc Software Consulting GmbH

3

Neulich in den Medien …

“Die deutsche Corona-App ist womöglich unter Gesichtspunkten des Datenschutzes Weltklasse, für eine effiziente Bekämpfung der Pandemie allerdings so gut wie unbrauchbar.”

Kommentar NZZ, 13.12.2020

Neue Zürcher Zeitung

4

Agenda

1 Einstieg und Motivation
2 Architekturrelevante Anforderungen
3 Lösungsansätze
4 Stärken, Risiken und Kompromisse
5 Ausblick und weitere Informationen

5

Agenda

1 **Einstieg und Motivation**
2 Architekturrelevante Anforderungen
3 Lösungsansätze
4 Stärken, Risiken und Kompromisse
5 Ausblick und weitere Informationen

1

6

Gemeinsam Corona bekämpfen

https://www.coronawarn.app

7

Warum ist die App so wichtig?

8

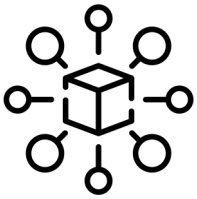
Wie funktioniert die App?

https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-erklaerfilm-1758828

9

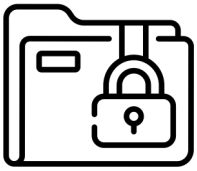
Was passiert mit den Daten?

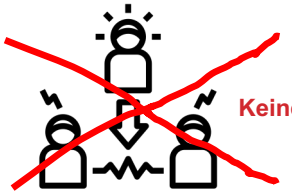
Keine Anmeldung



Dezentrale Speicherung

Keine Rückschlüsse auf persönliche Daten

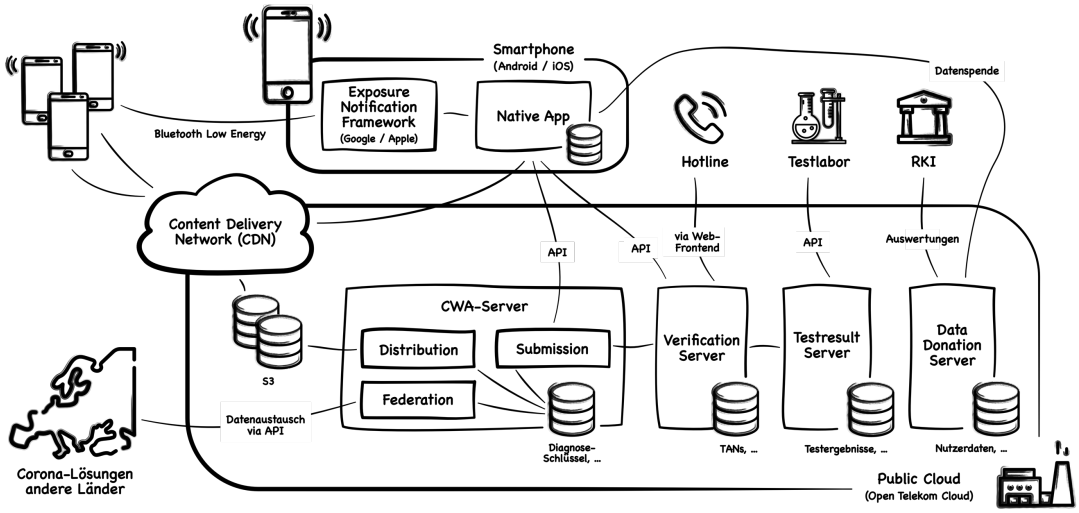




Keine Einsicht für Dritte

10

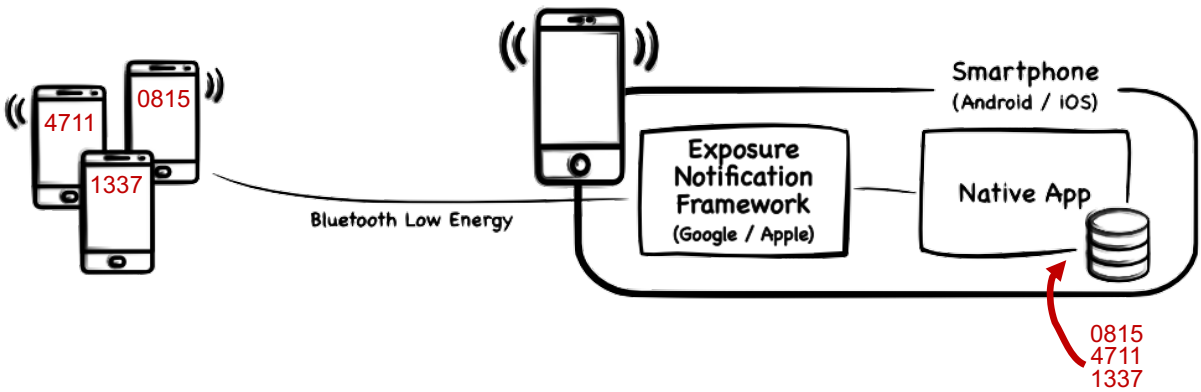
Architektur CWA: Informelles Überblicksbild



Quelle der Abbildung: S. Zörner, F. Sippach: „So gehen Architektur-Reviews! Entlang der Corona-Warn-App“, OOP 2021

11

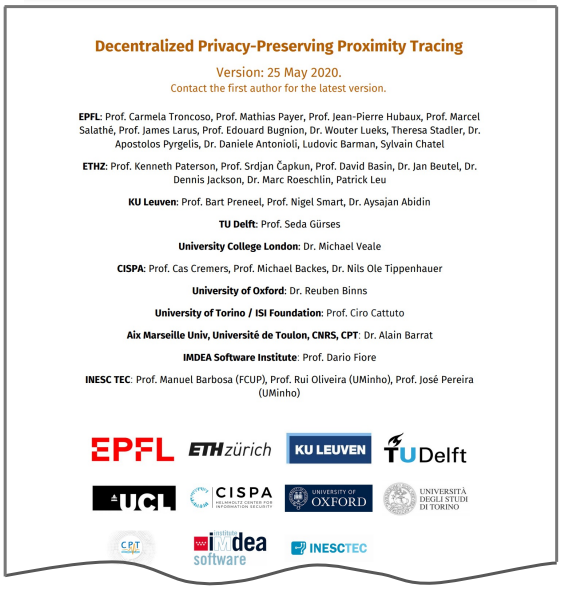
Austausch Tokens



12

Executive Summary

*This document describes and analyzes a system for **secure and privacy-preserving proximity tracing at large scale**. This system provides a technological foundation to help **slow the spread of SARS-CoV-2** by simplifying and accelerating the process of notifying people who might have been exposed to the virus so that they can take appropriate measures to break its transmission chain. The system aims to **minimise privacy and security risks for individuals and communities** and **guarantee the highest level of data protection**.*



Decentralized Privacy-Preserving Proximity Tracing

Version: 25 May 2020.

Contact the first author for the latest version.

EPFL: Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel

ETHZ: Prof. Kenneth Paterson, Prof. Srdjan Čapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

KU Leuven: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

TU Delft: Prof. Seda Gürses

University College London: Dr. Michael Veale

CISPA: Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer

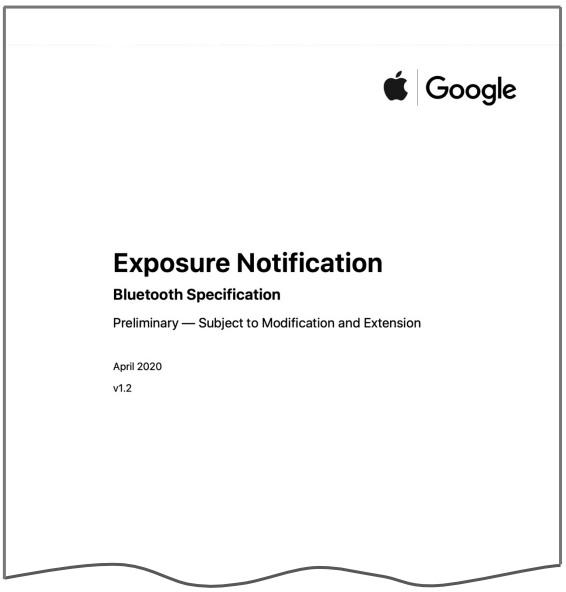
University of Oxford: Dr. Reuben Binns

University of Torino / ISI Foundation: Prof. Ciro Cattuto

Aix Marseille Univ, Université de Toulon, CNRS, CPT: Dr. Alain Barrat

IMDEA Software Institute: Prof. Dario Fiore

INESC TEC: Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)



Google

Exposure Notification

Bluetooth Specification

Preliminary — Subject to Modification and Extension

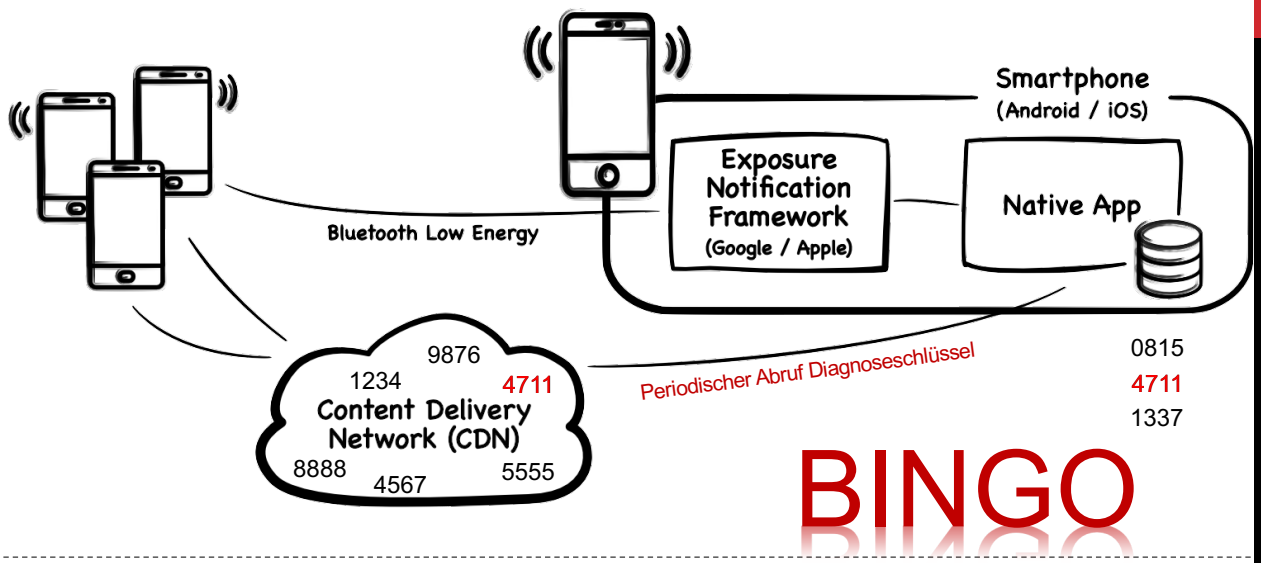
April 2020

v1.2

Overview

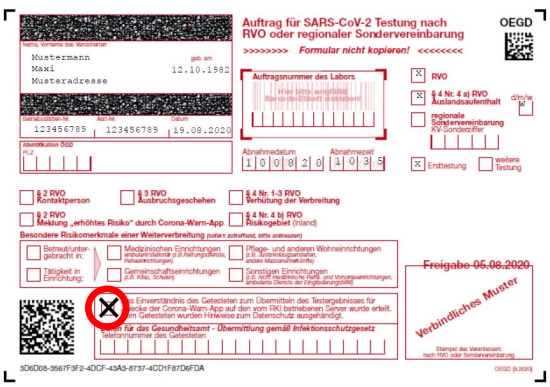
*This document provides the detailed technical **specification** for a **new privacy-preserving Bluetooth protocol** to support Exposure Notification. Exposure Notification makes it possible to combat the spread of the coronavirus — the pathogen that causes COVID-19 — by **alerting participants about possible exposure to someone they have recently been in contact with**, who has subsequently been positively diagnosed as having the virus. [..] uses the **Bluetooth Low Energy wireless technology for proximity detection of nearby smartphones**, and for the data exchange mechanism.*

Kontakt mit positiv Getesteten

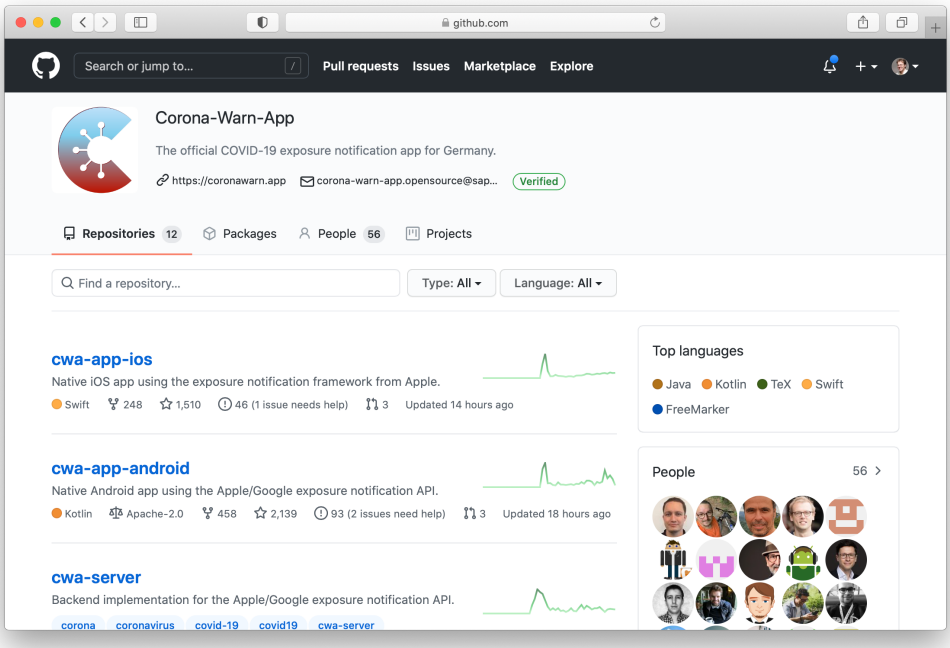


15

Funktionsweise: Testen lassen



16



17

Auftraggeber

Die Bundesregierung

Herausgeber

ROBERT KOCH INSTITUT

Entwicklung

SAP

Berater

Fraunhofer

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Bundesamt für Sicherheit in der Informationstechnik

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

18

Mission Statement (für diesen Vortrag)

- Klären, was **architekturrelevante Anforderungen** sind.
- Einblicke geben in die Architektur der **Corona-Warn-App**.
- **Stärken, Risiken und Kompromisse** der gewählten Architektur der CWA kennenlernen.

19

Agenda

1 Einstieg und Motivation
2 **Architekturrelevante Anforderungen**
3 Lösungsansätze
4 Stärken, Risiken und Kompromisse
5 Ausblick und weitere Informationen

2

20

Was ist Softwarearchitektur?

Softwarearchitektur :=

$\sum$ wichtige Entscheidungen

wichtig :=

- fundamental (betrifft viele)
- im weiteren Verlauf nur schwer zu ändern
- entscheidend für den Erfolg des Softwaresystems

21

Themen für Entscheidungen

Zerlegung

Welcher Architekturstil?
Wie zerfällt die Anwendung?
Teilsysteme, Module,
Komponentenbildung,
Abhängigkeiten ...

Zielumgebung

Wo läuft die Software?
Beim Endanwender, im
eigenen Rechenzentrum,
Cloud, Verteilung,
Virtualisierung ...

Technologie-Stack

Was setzen wir ein?
Programmiersprache(n)
Bibliotheken, Frameworks,
Middleware,
Querschnittsthemen ....

Vorgehen

Wie arbeiten wir?
Planen, Entwickeln, Testen,
Bauen, Dokumentieren,
Ausliefern, Nachjustieren,
...

22

CWA – Konkrete Entscheidungen

Zerlegung

Client/Server mit Apps und Backend-Server als verteilte Menge einzeln deploybarer Services, **fachlich zerlegt** (Test-ergebnisse, Verifikation …)

Zielumgebung

Clients: **Smartphones** der Endnutzer, Backend: **Kubernetes in der Telekom-Cloud** …

Technologie-Stack

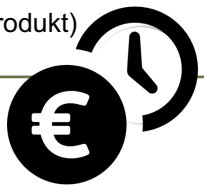
Native Apps in Swift und Kotlin auf iOS und Android.
Backend in **Java mit Spring Boot**, Postgres, …

Vorgehen

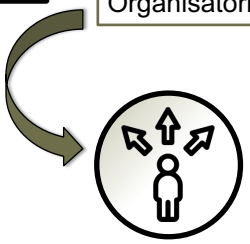
Entwicklung als **Open Source**, Quelltexte in **GitHub**, **Dokumentation** in Markdown, automatisierte **Tests**
...

Einflüsse auf Entscheidungen

Rahmenbedingungen
Technisch (z.B. Datenbankprodukt)
Organisatorisch (z.B. Team)



- schränken die Lösung ein
- schließen Optionen aus



Zentrale Rahmenbedingungen Corona-Warn-App

Technisch

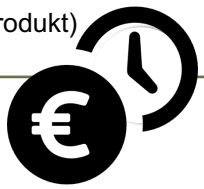
- Betrieb in der **Cloud**
- **Native mobile** Clients
- Einsatz des **Exposure Notification Framework**

Organisatorisch

- **Große Medienaufmerksamkeit**, gewisse **Skepsis** am Mehrwert innerhalb der Bevölkerung
- Konsortium aus **zwei Auftragnehmern** (SAP und Deutsche Telekom)
- **Enger Zeitrahmen**
- Hoher **politischer Druck**, viele Parteien involviert (Ministerien, Behörden, RKI)
- **Hohe Datenschutzanforderungen**

Einflüsse auf Entscheidungen

Rahmenbedingungen
Technisch (z.B. Datenbankprodukt)
Organisatorisch (z.B. Team)



- schränken die Lösung ein
- schließen Optionen aus

- prägen die Lösung
- nachher schwierig "einzubauen"

Qualitätsanforderungen
Benutzbarkeit, Effizienz,
Wartbarkeit, Sicherheit ...

Qualitätsmerkmale

Begriffe nach ISO 25010

Benutzbarkeit (Usability)
Ist die Software intuitiv zu bedienen, leicht zu erlernen, attraktiv?

Portabilität (Portability)
Ist die Software leicht auf andere Zielumgebungen (z.B. anderes OS) übertragbar?

Funktionale Eignung (Functional Suitability)
Sind die berechneten Ergebnisse genau genug / exakt, ist die Funktionalität angemessen? ...

Effizienz (Performance)
Antwortet die Software schnell, hat sie einen hohen Durchsatz, einen geringen Ressourcenverbrauch? ...

Kompatibilität (Compatibility)
Ist die Software konform zu Standards, arbeitet sie gut mit anderen zusammen?

Zuverlässigkeit (Reliability)
Ist das System verfügbar, tolerant gegenüber Fehlern, nach Abstürzen schnell wieder hergestellt? ...

Sicherheit (Security)
Ist das System sicher vor Angriffen? Sind Daten und Funktion vor unberechtigtem Zugriff geschützt? ...

Wartbarkeit (Maintainability)
Ist die Software leicht zu ändern, erweitern, testen, verstehen? Lassen sich Teile wiederverwenden? ...

27

Top-Qualitätsziele Corona-Warn-App

	Ziel	Beschreibung
	Höchster Datenschutz	Der Schutz der personenbezogenen Daten hat oberste Priorität. *(Sicherheit)*
	Effektive Warnfunktionalität	Die App ist ein effektiver Baustein bei der Pandemie-Bekämpfung. *(Funktionale Eignung)*
	Attraktive Lösung für App-Nutzer	Die App ist leicht zu installieren sowie intuitiv und effizient zu bedienen. *(Benutzbarkeit)*
	Hohe Zuverlässigkeit	Die Lösung geht mit Lastspitzen wegen hoher Nutzer- oder Infektionszahlen ebenso souverän um, wie mit böswilligen Angriffen. *(Zuverlässigkeit)*
	Gute Änderbarkeit	Die Software lässt sich leicht anpassen, wenn z. B. Nutzer/-innen oder neue Forschungsergebnisse es erfordern. *(Wartbarkeit/Erweiterbarkeit)*

Die Reihenfolge gibt Orientierung bezüglich der Wichtigkeit.

28

Agenda

1 Einstieg und Motivation
2 Architekturrelevante Anforderungen
3 **Lösungsansätze**
4 Stärken, Risiken und Kompromisse
5 Ausblick und weitere Informationen

3

29

Mission Statement

Die **Corona-Warn-App** ist eine App, die hilft, **Infektionsketten** des SARS-CoV-2 (COVID-19-Auslöser) in Deutschland **nachzuverfolgen** und zu **unterbrechen**.

Die App basiert auf Technologien mit einem **dezentralisierten Ansatz** und informiert Personen, wenn sie mit einer infizierten Person in Kontakt standen.

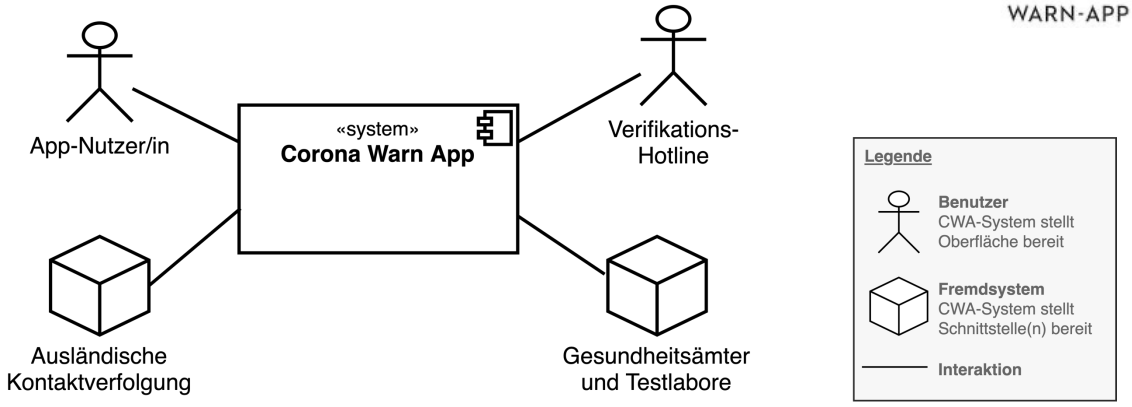
Transparenz ist von entscheidender **Bedeutung**, um die Bevölkerung zu schützen und die **Akzeptanz zu erhöhen**.

Quelle: https://www.coronawarn.app/de/

30

Kontextabgrenzung

Dieser fachliche Systemkontext zeigt das Corona-Warn-App-System im Zusammenspiel mit den wichtigsten Benutzern und Fremdsystemen.



31

Fachlicher Systemkontext, Akteure

Kurze Erläuterungen zu den Benutzern und Fremdsystemen

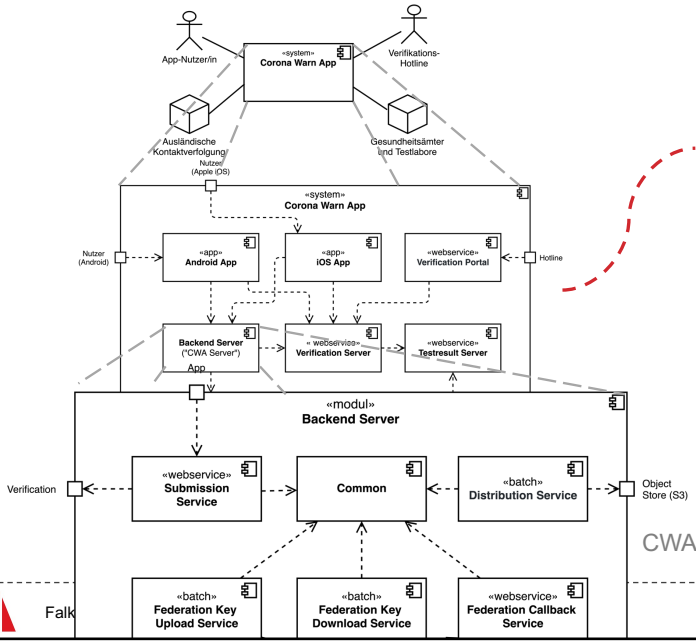
Akteur	Beschreibung
App-Nutzer/in	Erhält Informationen über mögliche Begegnungen mit infizierten Personen und eigene Testergebnisse. Verifiziert eigene Testergebnisse und warnt so freiwillig andere.
Verifikations-Hotline	Unterstützt App-Nutzer/innen bei der Freischaltung positiver Testergebnisse (“teleTAN").
Gesundheitsämter und Testlabore	Liefern anonymisierte Testergebnisse an das System.
Ausländische Kontaktverfolgungen	Austausch mit dezentralen Anwendungen anderer Länder zur grenzüberschreitenden Ermittlung von Kontakten.

32

Lösungsstrategie Corona-Warn-App

	Ziel	Passende Lösungsansätze (Auswahl)
	Höchster Datenschutz	• Speicherung der **Daten lokal** • **Verschlüsselung** aller Bewegungsdaten • Senden der Daten nur **nach Aufforderung** • **Transparente** Entwicklung (Open Source)
	Effektive Warnfunktionalität	• Verwendung **Exposure Notification Framework** • **Digitale Abläufe** bevorzugt • Optionales, manuelles **Kontakt-Tagebuch**
	Attraktive Lösung für App-Nutzer	• **Native Clients** (L&F) • **Übersichtliche** Gestaltung und **simple** Bedienung
	Hohe Zuverlässigkeit	• **Microservices,** Docker, Kubernetes, **Public Cloud** • hohe **Testabdeckung** und **automatisierte Builds** • Bereitstellung von zu lesenden Daten über **CDN**
	Gute Änderbarkeit	• Hoher **Modularisierungsgrad** • **Open Source** Projekt, gute **Dokumentation** • Verwendung von **Standard** & **Open Source** Libraries • Konsortium von **mehreren Auftragnehmern** • **Code-Qualität** (SonarQube, SwiftLint, Checkstyle, …)

Tatsächliche Zerlegung im Quelltext



„Bausteinsicht, Ebene 1"

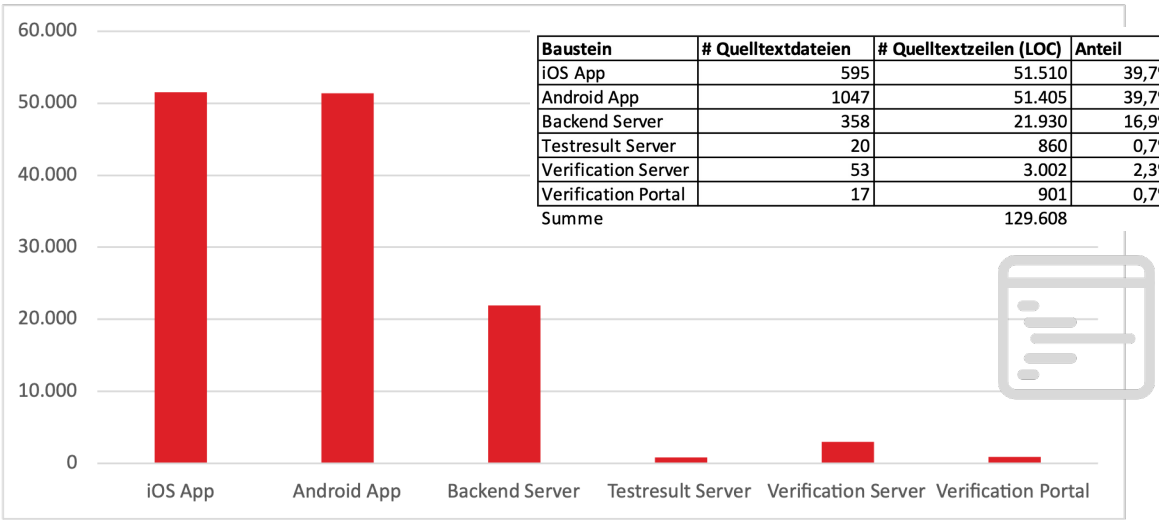
GitHub-Repositories

https://github.com/corona-warn-app/...

- cwa-app-android
- cwa-app-ios
- cwa-server („Backend")
- cwa-testresult-server
- cwa-verification-server
- cwa-verification-portal

CWA-Server (Backend), Bausteinsicht, Ebene 2

Umfang je Baustein auf Ebene 1



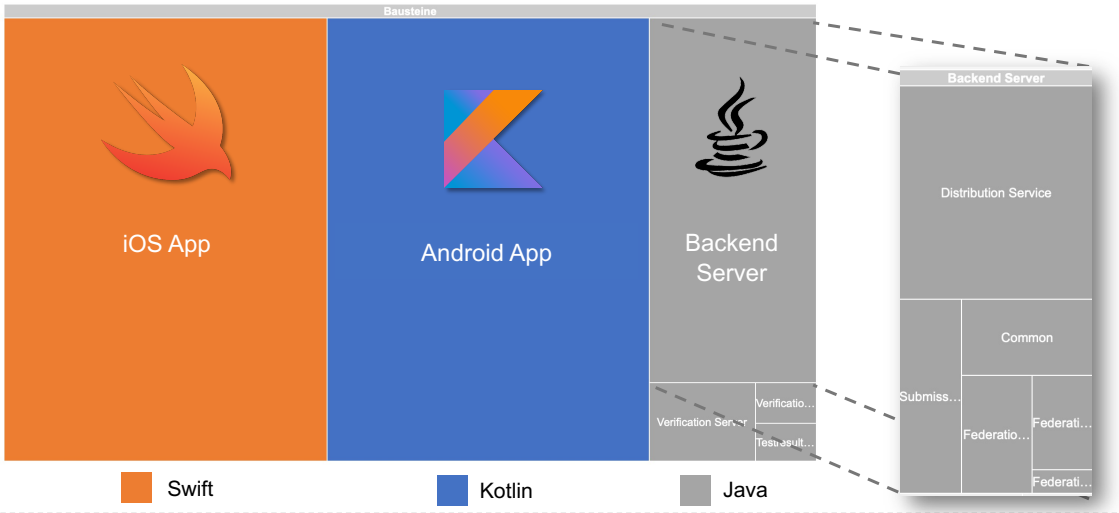
Baustein	# Quelltextdateien	# Quelltextzeilen (LOC)	Anteil
iOS App	595	51.510	39,7%
Android App	1047	51.405	39,7%
Backend Server	358	21.930	16,9%
Testresult Server	20	860	0,7%
Verification Server	53	3.002	2,3%
Verification Portal	17	901	0,7%
Summe		129.608	

Ermittelt mit Teamscale am 29.01.2021, nur Quelltext (Kotlin, Swift, Java), inklusive Tests

35

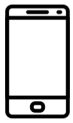
Treemap zum Umfang inkl. Programmiersprachen

Die Fläche einer Kachel entspricht LOCs des Repositories, die Farbe der Programmiersprache.



36

Technologie-Stack



- **Native Clients** in Swift bzw. Kotlin für iOS und Android
- **SQLite**

- **Java 11**
- **Spring Boot/Cloud/Data**
- Lombok, Guava, …
- **REST**, **Protobuf**
- **OpenAPI**, Micrometer
- Liquibase

- Maven, Gradle
- **Docker, Kubernetes**
- **Open Telekom Cloud** (OpenStack)
- PostgreSQL, **S3**, **CDN**
- Keycloak

37

Agenda

1 Einstieg und Motivation
2 Architekturrelevante Anforderungen
3 Lösungsansätze
4 **Stärken, Risiken und Kompromisse**
5 Ausblick und weitere Informationen

4

38

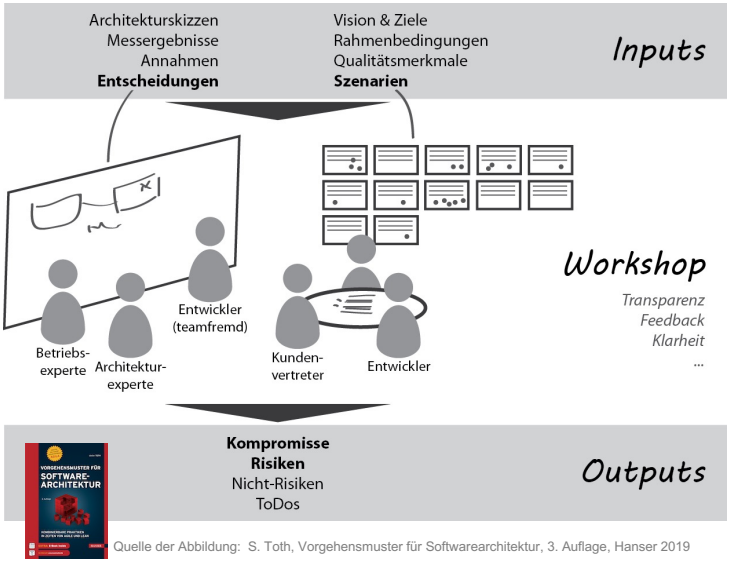
Szenarienbasierte Bewertung

Ablauf

(1) Szenarien generieren

(2) Szenarien priorisieren

(3) Szenarien durchsprechen
(der Reihe, nach Priorität)



Quelle der Abbildung: S. Toth, Vorgehensmuster für Softwarearchitektur, 3. Auflage, Hanser 2019

Was ist ein Szenario?

Ein Qualitätsszenario (auch: Bewertungsszenario) ...

- ... ist ein kurzer Text (1-3 Sätze).
- ... beschreibt **beispielhaft** die Verwendung des Systems, und zwar so dass ein **Qualitätsmerkmal** die Hauptrolle spielt.

Wie konkret?

Man muss sinnvoll drüber reden können.
Man muss es (theoretisch) überprüfen können.
(Kein Abnahmekriterium, kein Testfall!)

Brainstorming – analog oder digital

In Präsenz:
Post-its

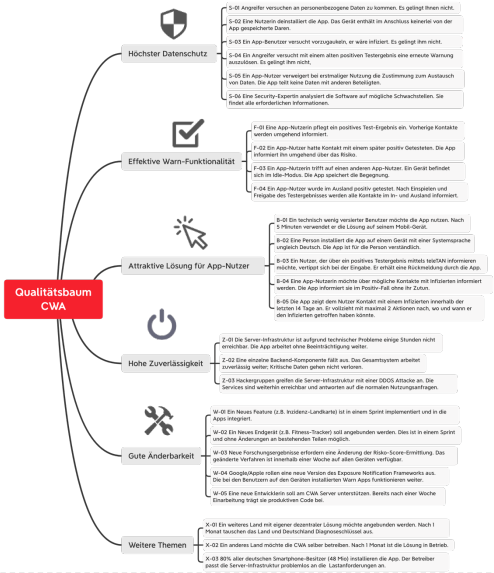
Remote:
Digitale Whiteboards
(miro, Mural, …)

miro

MURAL

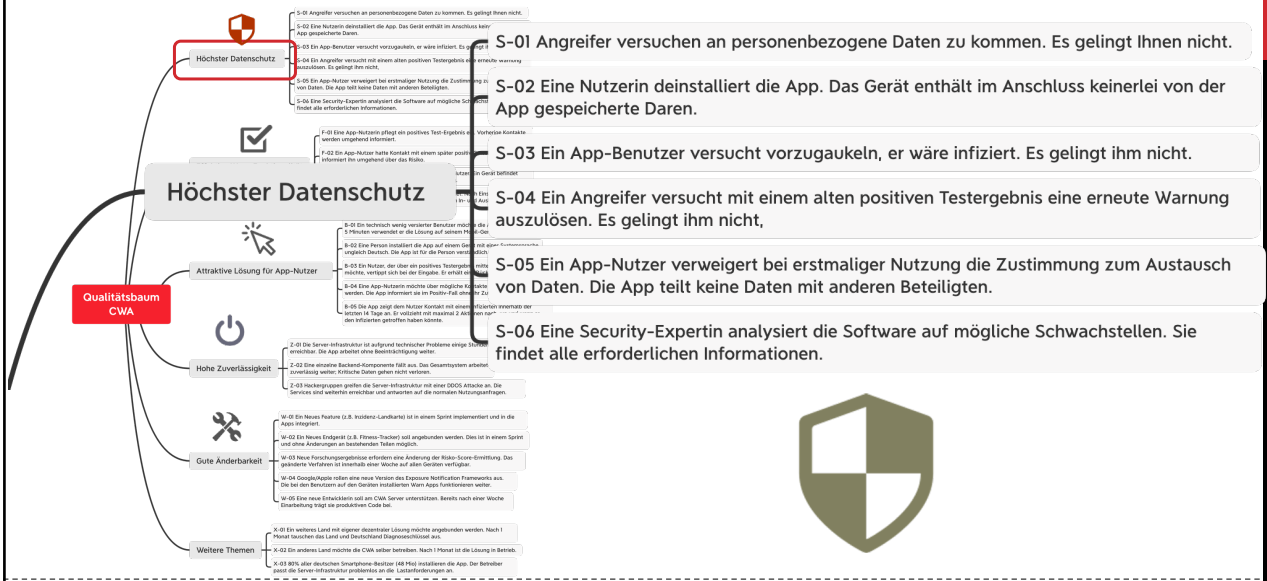
41

Ergebnis: Qualitätsbaum mit Szenarien



42

Ergebnis: Qualitätsbaum mit Szenarien



S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

S-02 Eine Nutzerin deinstalliert die App. Das Gerät enthält im Anschluss keinerlei von der App gespeicherte Daren.

S-03 Ein App-Benutzer versucht vorzugaukeln, er wäre infiziert. Es gelingt ihm nicht.

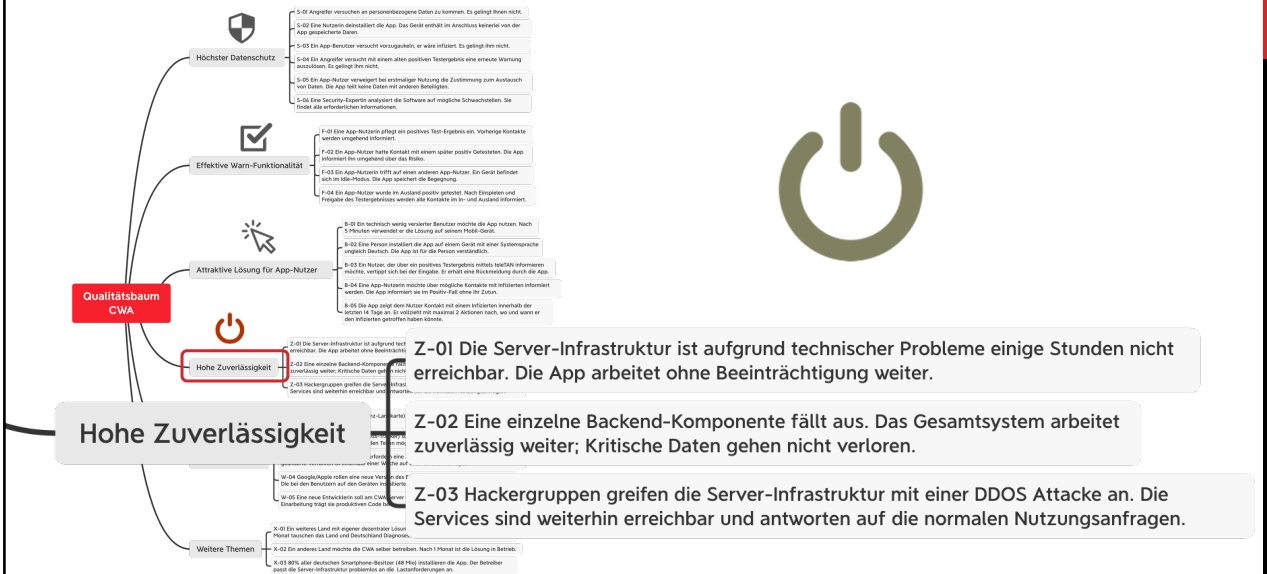
S-04 Ein Angreifer versucht mit einem alten positiven Testergebnis eine erneute Warnung auszulösen. Es gelingt ihm nicht,

S-05 Ein App-Nutzer verweigert bei erstmaliger Nutzung die Zustimmung zum Austausch von Daten. Die App teilt keine Daten mit anderen Beteiligten.

S-06 Eine Security-Expertin analysiert die Software auf mögliche Schwachstellen. Sie findet alle erforderlichen Informationen.

43

Ergebnis: Qualitätsbaum mit Szenarien



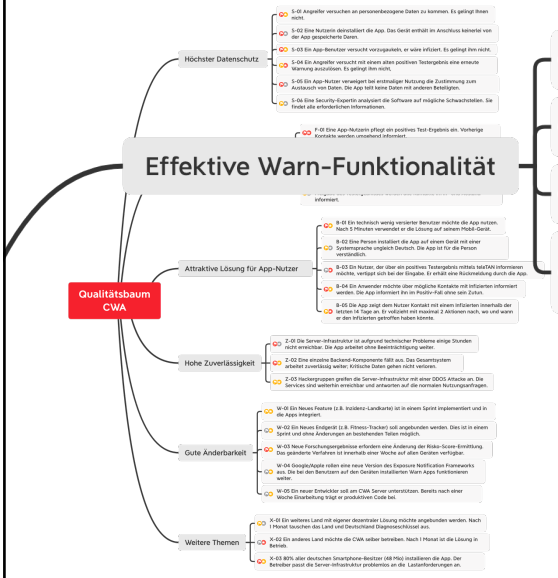
Z-01 Die Server-Infrastruktur ist aufgrund technischer Probleme einige Stunden nicht erreichbar. Die App arbeitet ohne Beeinträchtigung weiter.

Z-02 Eine einzelne Backend-Komponente fällt aus. Das Gesamtsystem arbeitet zuverlässig weiter; Kritische Daten gehen nicht verloren.

Z-03 Hackergruppen greifen die Server-Infrastruktur mit einer DDOS Attacke an. Die Services sind weiterhin erreichbar und antworten auf die normalen Nutzungsanfragen.

44

Beispiel: Unser CWA-Qualitätsbaum, priorisiert



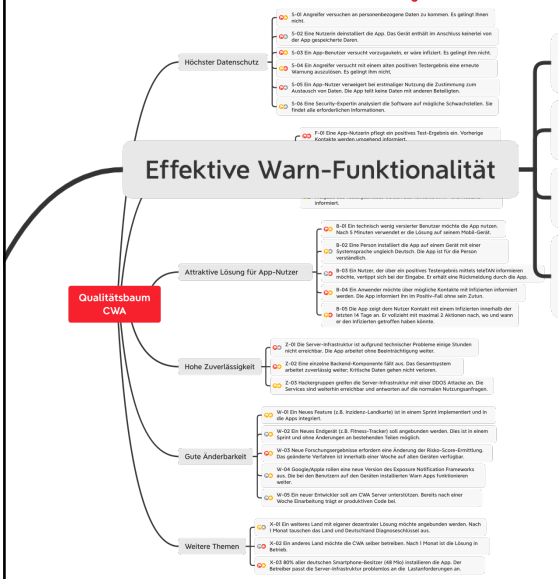
- F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.
- F-02 Ein App-Nutzer hatte Kontakt mit einem später positiv Getesteten. Die App informiert ihn umgehend über das Risiko.
- F-03 Ein App-Nutzerin trifft auf einen anderen App-Nutzer. Ein Gerät befindet sich im Idle-Modus. Die App speichert die Begegnung.
- F-04 Ein App-Nutzer wurde im Ausland positiv getestet. Nach Einspielen und Freigabe des Testergebnisses werden alle Kontakte im In- und Ausland informiert.

Legende für Priorität

- Fachliche Wichtigkeit
- Technische Schwierigkeit
- Rot: Hoch
- Gelb: Mittel
- Grau: Niedrig

45

Szenario „rauspicken": F-01

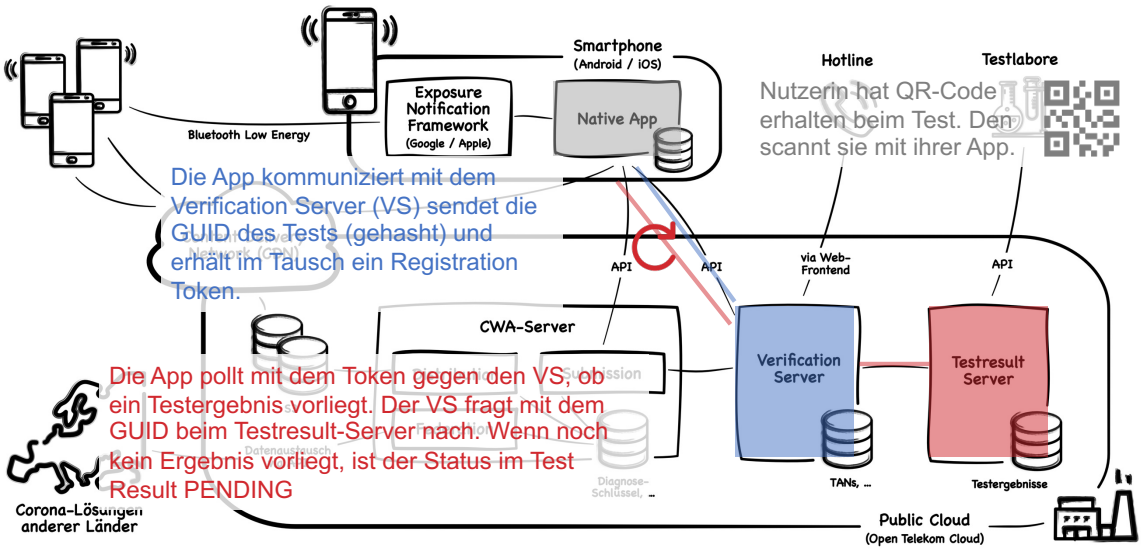


- F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.
- F-02 Ein App-Nutzer hatte Kontakt mit einem später positiv Getesteten. Die App informiert ihn umgehend über das Risiko.
- F-03 Ein App-Nutzerin trifft auf einen anderen App-Nutzer. Ein Gerät befindet sich im Idle-Modus. Die App speichert die Begegnung.
- F-04 Ein App-Nutzer wurde im Ausland positiv getestet. Nach Einspielen und Freigabe des Testergebnisses werden alle Kontakte im In- und Ausland informiert.

F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.

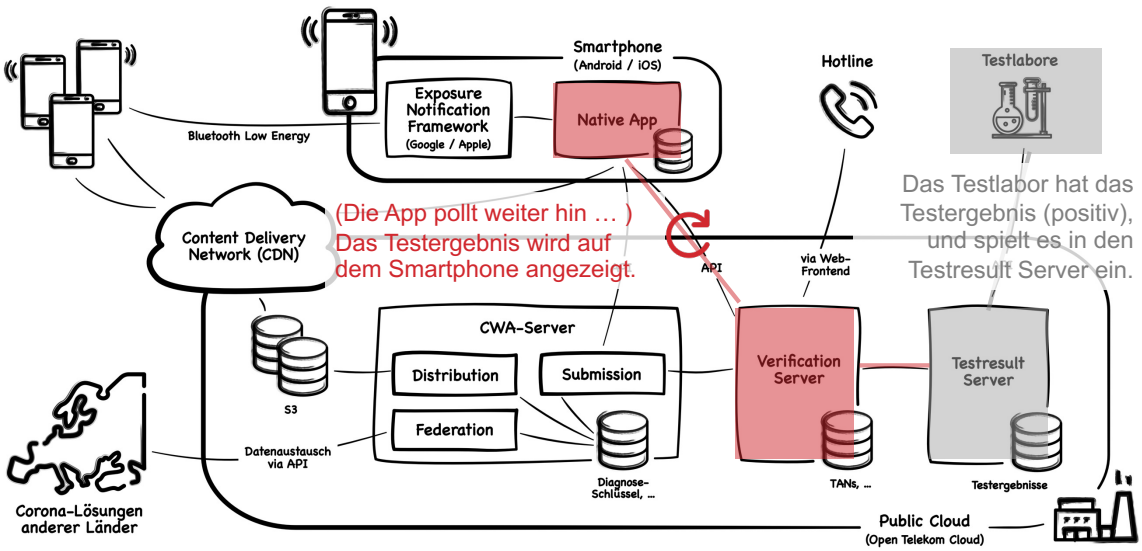
46

Szenario F-01: Schritte entlang des Überblicks



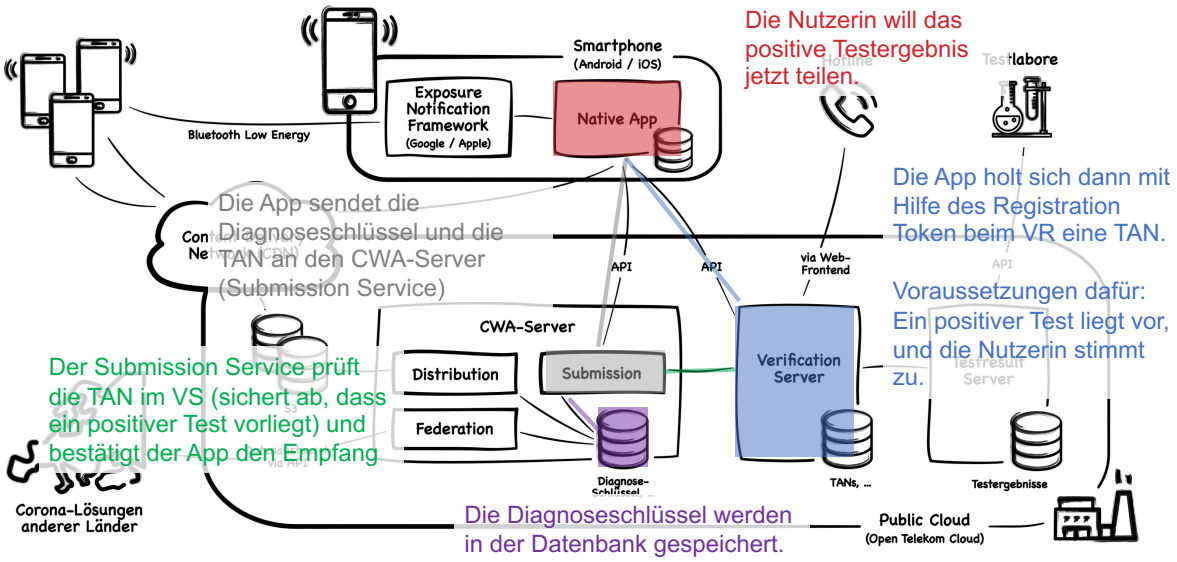
47

Szenario F-01: Schritte entlang des Überblicks



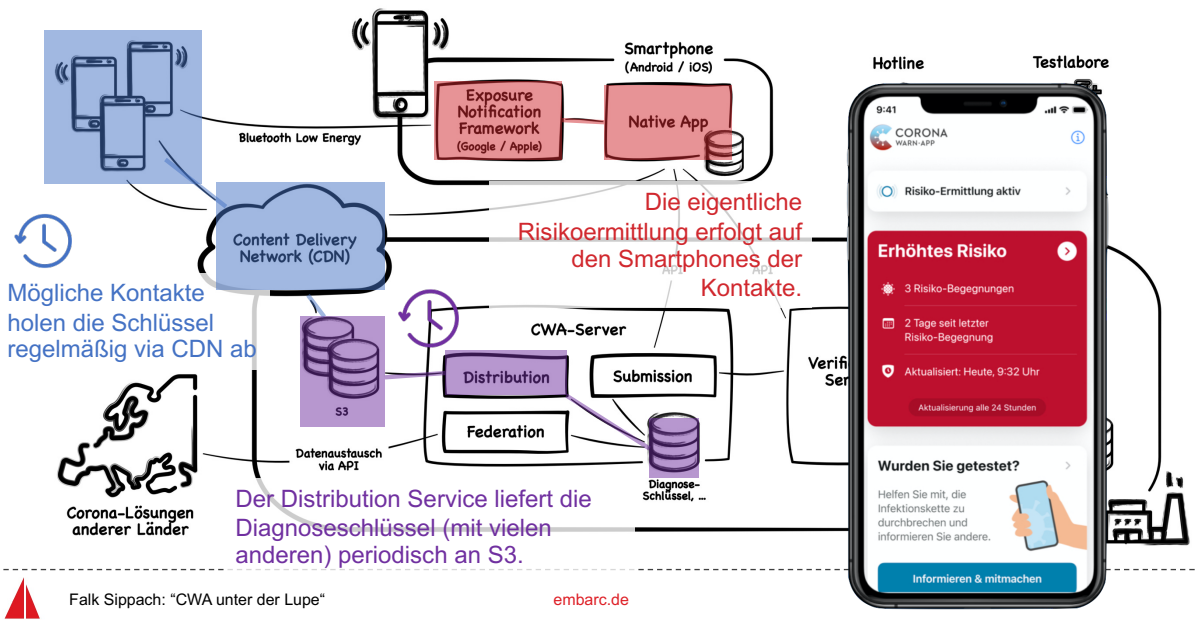
48

Szenario F-01: Schritte entlang des Überblicks



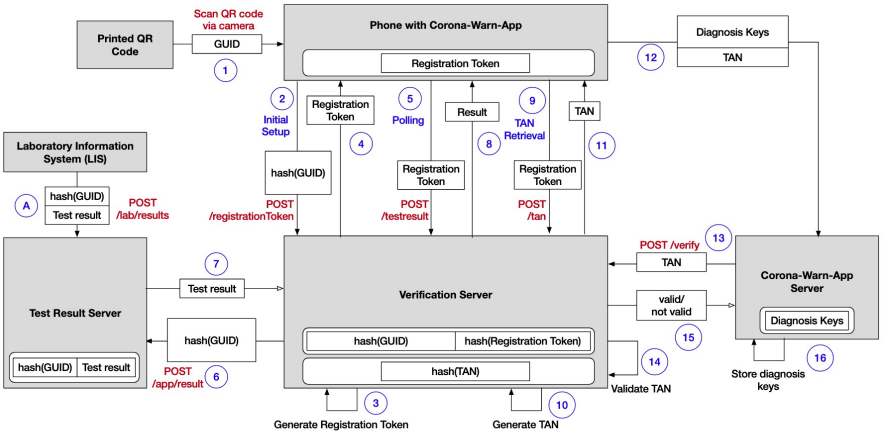
49

Szenario F-01: Schritte entlang des Überblicks



50

Zum ganz genau nachlesen …



Data flow for the verification process

https://github.com/corona-warn-app/cwa-verification-server/blob/master/docs/architecture-overview.md

Ausgewählte Ergebnisse zu Szenario F-01

F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.

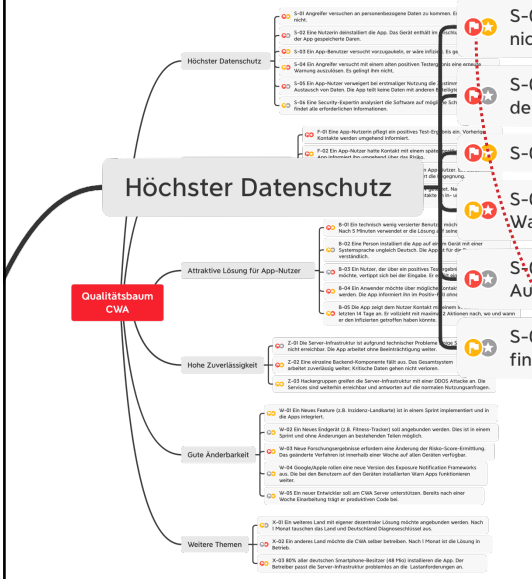
Kompromisse

- Apps der Kontakte aktualisieren via CDN nur ab und an
  (+) **effiziente Nutzung / Bandbreite** des Smartphone
  (-) nicht "umgehend", **Verzögerung bei Warnungen**
- explizite Einwilligung der Nutzerin erforderlich
  (-) **Benutzbarkeit**
  (+) **Datenschutz**
- Registration Token und TAN „verkomplizieren" den Ablauf
  (TAN wichtig für Sicherheits-Szenarien S-03 und S-04)

Risiken

- Wenn das Testlabor das Ergebnis nicht oder **zeitlich stark verzögert einspielt**, kann die Nutzerin erst **spät freigeben**, oder gar nicht, oder **gibt irgendwann resigniert auf**.
- Periodische Erzeugung der Daten kann Liefern der Diagnoseschlüssel an S3 verzögern (gefährdet „umgehend") – Fragen: Wie oft passiert das? Wie lange dauert ein Lauf?

Szenario 2: S-01



S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

S-02 Eine Nutzerin deinstalliert die App. Das Gerät enthält im Anschluss keinerlei von der App gespeicherte Daren.

S-03 Ein App-Benutzer versucht vorzugaukeln, er wäre infiziert. Es gelingt ihm nicht.

S-04 Ein Angreifer versucht mit einem alten positiven Testergebnis eine erneute Warnung auszulösen. Es gelingt ihm nicht,

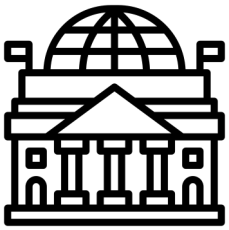
S-05 Ein App-Nutzer verweigert bei erstmaliger Nutzung die Zustimmung zum Austausch von Daten. Die App teilt keine Daten mit anderen Beteiligten.

S-06 Eine Security-Expertin analysiert die Software auf mögliche Schwachstellen. Sie findet alle erforderlichen Informationen.

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

Szenario 2 (S-01): Nachschärfen

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.



Wer “greift an“?

Gute oder schlechte Absichten?

Szenario 2 (S-01): Nachschärfen

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

Was sind personen-bezogene Daten?

- "Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen". (**Artikel 4 DSGVO**)
- **Identifiziert** = Zuordnung der Daten ohne Umweg, direkter Bezug herstellbar
- **Identifizierbar** = Zuordnung mit Zusatzwissen

Wer nutzt die App überhaupt?

- 22 Millionen Installationen der App
- **18 bis 20 Millionen** aktive Nutzer
- mehr als **zwei Millionen Laborergebnisse** über die App übermittelt
- rund **53.000 Nutzer** haben ihr positives Testergebnis **über die App geteilt**.

Laut Bundesregierung (November 2020)

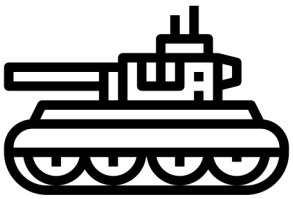
55

Szenario 2 (S-01): Nachschärfen

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

Potentielle Angriffsvektoren (in der Theorie!)

ID-Scanner



ID-Bomber

ID-Repeater

56

Szenario 2 (S-01): **Nachschärfen**

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

Was darf nicht passieren?

Personen tracken

Falschmeldungen verbreiten

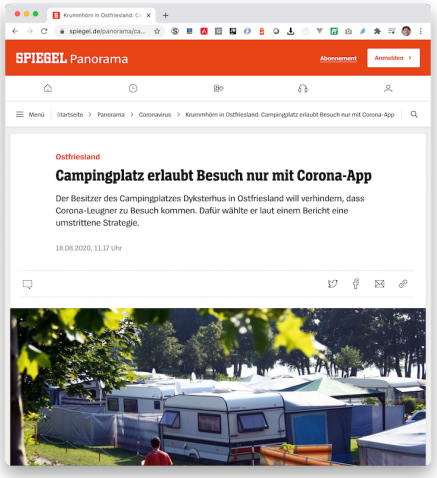
Verpflichtung zur App an bestimmten Orten und Veranstaltungen

Namen von Infizierten ermitteln

Gesundheitsamt wird direkt über erhöhtes Risiko informiert und ordnet Quarantäne an

57

CWA als Must-Have?

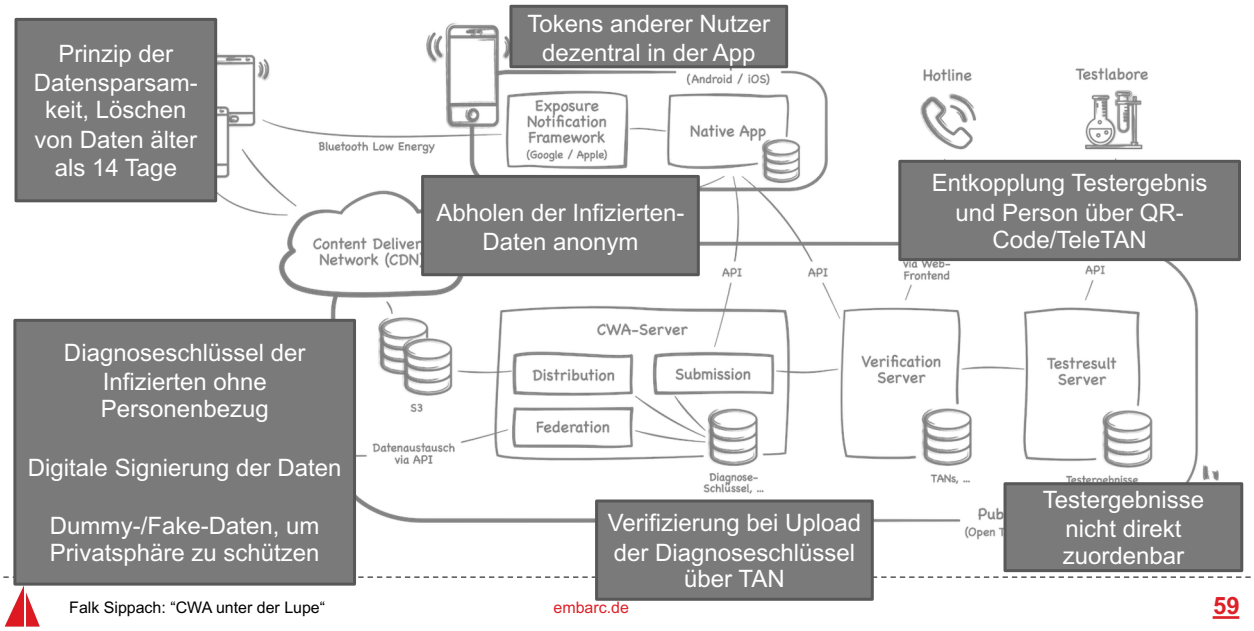


*„Nur wer die Corona-Warn-App installiert hat, **darf anreisen**: Ein Betreiber eines Campingplatzes in Niedersachsen versucht ab diesem Dienstag mit einer drastischen Strategie, **Urlauber fernzuhalten**, die aus seiner Sicht das **Coronavirus nicht ernst nehmen**. Angesichts der steigenden Zahl der Infizierten wolle er seine **Gäste, seine Familie und sich selbst schützen**, sagte Campingplatz-Chef […]"*

https://www.spiegel.de/panorama/camping-platz-erlaubt-besuch-nur-mit-corona-app-a-0c6bfcfe-5bcb-463a-b670-790030560d80#

58

Szenario S-01: Wo/Wie werden Daten gespeichert?



59

Ausgewählte Ergebnisse zu Szenario S-01

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

Stärken

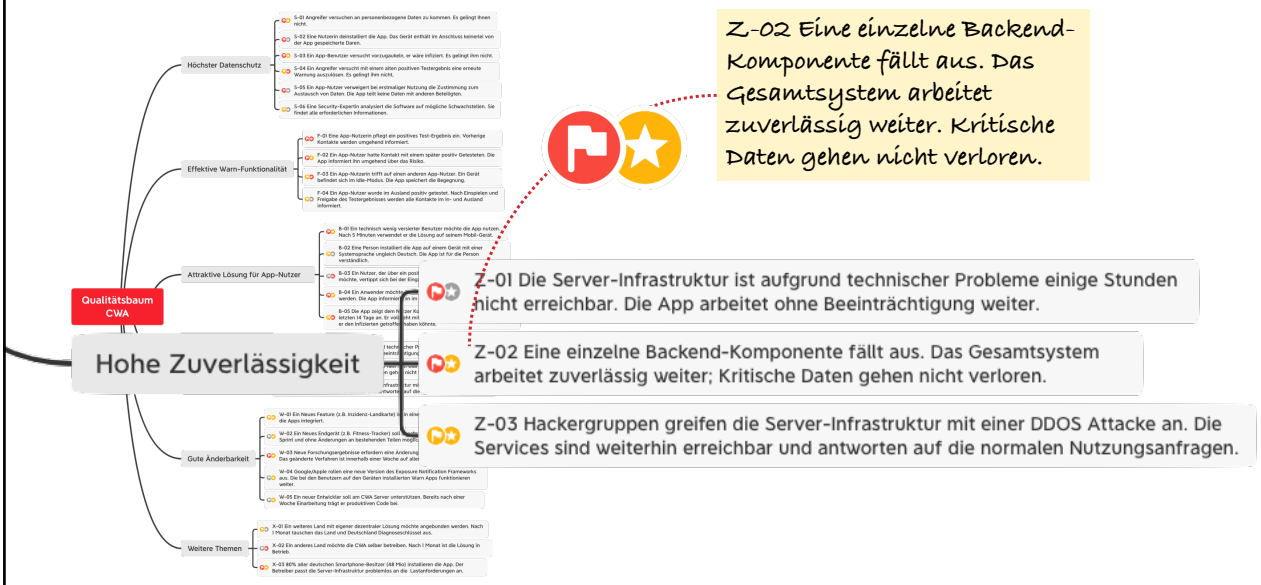
+ **Dezentrale Speicherung** auf den Smartphones
+ **Datensparsamkeit** (keine direkte Speicherung von personenbezogenen Daten)
+ **Regelmäßige Löschen** (14 Tage)
+ **Fake-Daten**, um bei geringer Datenmenge keine Rückschlüsse zu erlauben
+ Generierung von Schlüsseln, **rollierende Tokens**

Kompromisse

- Offenlegung des Quelltextes
  (+) **schafft Vertrauen**
  (-) **zeigt** ggf. **Schwachstellen** auf
- Gesundheitsämter haben keinen direkten Zugriff auf personenbezogene Daten
  (+) **keine** Bevormundung/**Überwachung**
  (-) Staat ist auf **freiwillige Mithilfe** angewiesen
- Keine Möglichkeit, in den letzten Tagen getroffene Personen zu ermitteln (Pull, kein Push)
  (-) Kontakte muss jeder **selbst dokumentieren**
  (+) CWA bietet ein digitales Kontakt-Tagebuch an
- Wirksamkeit wegen hohen Datenschutzanforderungen zu gering?
  (+) **Chaos Computer Club lobt** die CWA explizit
  (-) Politiker möchten den **Datenschutz** für eine bessere Wirkung **opfern**
- eingeschränkte Möglichkeiten zur Auswertung der Benutzung
  (+) **Datenschutz**
  (-) **Interessante Statistiken** zur Nutzung **nicht möglich**

60

Szenario 3: Z-02



61

Ausgewählte Ergebnisse zu Szenario Z-02

Z-02 Eine einzelne Backend-Komponente fällt aus. Das Gesamtsystem arbeitet zuverlässig weiter. Kritische Daten gehen nicht verloren.

Stärken

+ Apps funktionieren auch **ohne Backends** (sammeln Daten)
+ **“Kleine“ Services** mit meist eigener Datenhaltung
+ **Containerisierung** der Services und Orchestrierung über Kubernetes
+ **Public Cloud** inklusive horizontale Skalierbarkeit und Redundanz
+ Häufige Lesezugriffe über **CDN entkoppelt** (Caching, Skalierbarkeit)

Kompromisse

- Synchrone Kommunikation App zum Server
  (+) Benutzer erhalten **sofort Rückmeldung**
  (-) hat ggf. **Auswirkungen auf Zuverlässigkeit**
- Synchrone Kommunikation Labore zum Test-Result-Server
  (+) **einfacher aufzurufen** für die Labore
  (-) **Akzeptanz bei Benutzern sinkt**, wenn die Ergebnisse nicht in der App angezeigt werden

62

Agenda

1 Einstieg und Motivation

2 Architekturrelevante Anforderungen

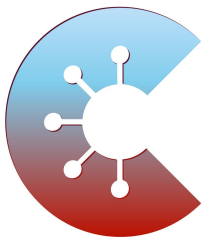
3 Lösungsansätze

4 Stärken, Risiken und Kompromisse

5 **Ausblick und weitere Informationen**

5

63



Gemeinsam Corona bekämpfen

https://www.coronawarn.app

64

Stetige Weiterentwicklung

Veranstaltungen, Restaurantbesuche

Anzeige der aktuellen Zahlen, freiwilliges Senden von Daten zu statistischen Zwecken

Einkaufen

Digitaler Impfausweis

65

Video-Tipp zur Corona-Warn-App

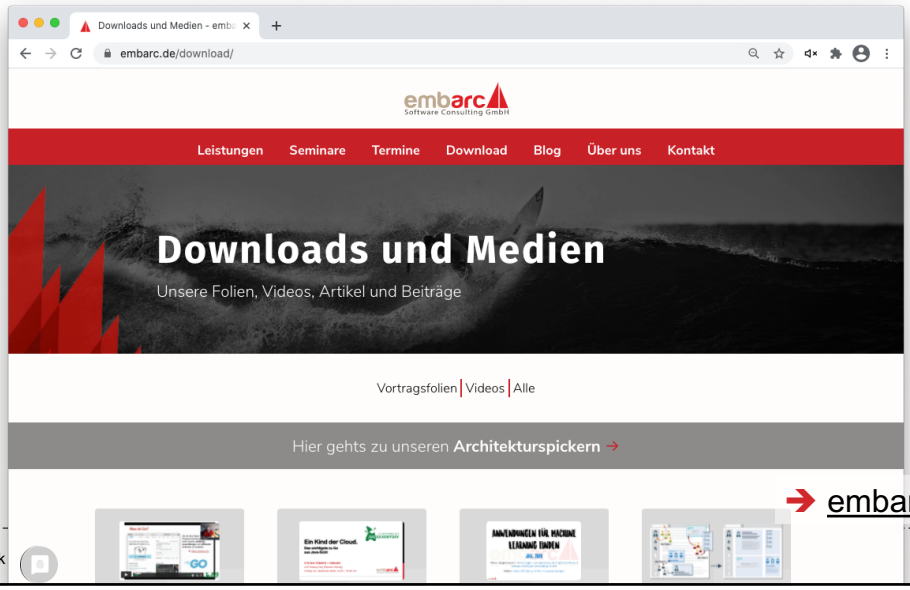
Video-Serie zur Funktionsweise der CWA von Thomas Bayer auf YouTube.

„Technischer Blick auf die Corona Warn App und ihre Backend-Systeme. Videos zur Funktionsweise, Softwarearchitektur, Protokollen, Sicherheit.“

#1: Wie funktioniert die Corona Warn App (CWA)?
https://www.youtube.com/watch?v=MEQ0wzk1Cp8
#2: Softwarearchitektur der Corona App
https://www.youtube.com/watch?v=ytglSxeTPyU
#3: Kommunikation mit Backend-Servern in der Cloud #1
https://www.youtube.com/watch?v=RKoBcsCA5ts
#4: Corona App Technik: Backend, Datenbank, S3, Cloud Teil #2
https://www.youtube.com/watch?v=7mebVNWcGxU

66

Folien von heute als PDF zum Download

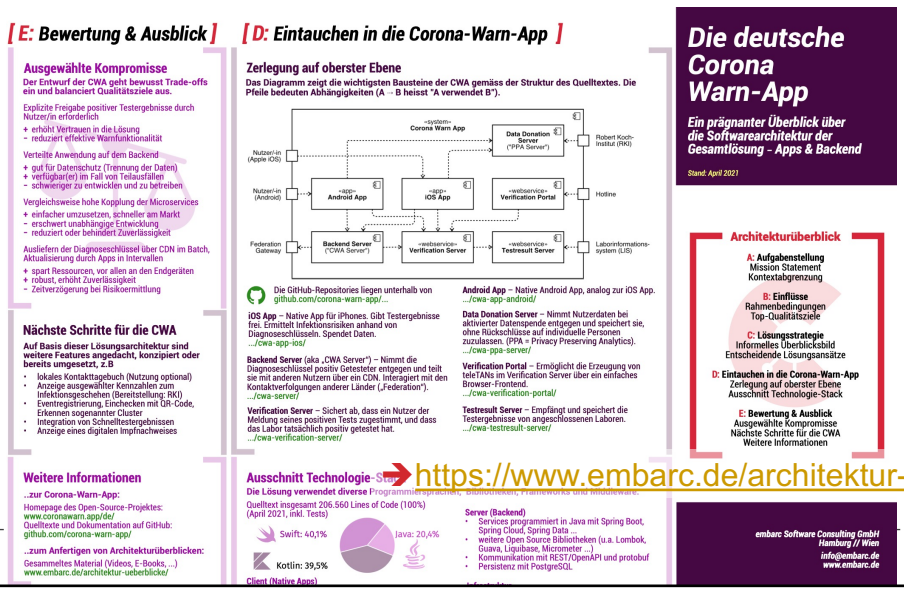


PDF

➔ embarc.de/download/

67

Flyer Architekturüberblick zur CWA zum Download



PDF

➔ https://www.embarc.de/architektur-ueberblicke/#cwa

68

Vielen Dank.

Ich freue mich auf Eure Fragen!

Falk Sippach

fs@embarc.de

@sippsack

➔ xing.to/fsi